## DETAILED ACTION

1. The response of 6/22/2011 was received and considered.

2. Claims 39, 41-50, 52-57, 59-69 and 71-77 are pending.

## EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with David Longo, 53,235, on 6/27/2011.

The application has been amended as follows:

In **CLAIM 39, LINE 10**, please **REPLACE** "information on" with "information relating to".

In **CLAIM 76, LINE 2**, please **DELETE** ", associated therewith".

In **CLAIM 77, PLEASE REPLACE THE CLAIM** with the following:

77. A non-transitory computer-readable storage medium encoded with a computer program product loadable into a memory of at least one computer, the computer program product containing software code portions for performing, when the computer program product is run on the at least one computer, a method of providing intrusion detection in a network wherein data flows are exchanged using associated network ports and application layer protocols, comprising the steps of:

monitoring data flows in said network;

detecting information relating to application layer protocols associated with said monitored data flows independently of said network ports; and

providing intrusion detection on said monitored data flows based on said detected information relating to said application layer protocols independently of any predefined association between said network ports and said application layer protocols,

wherein said step of detecting information relating to application layer protocols involved in said data flows comprises characterizing and classifying data flows related to each server application in said network.

***Allowable Subject Matter***

4. The following is an examiner's statement of reasons for allowance:

a. Regarding claims 39, 57, 76 and 77, the art of record teaches determining a server running (Roesch, col. 14, lines 42-44; Graham teaches determining FTP, Fig. 5). However, the prior art of record fails to teach or disclose, either alone or in combination, characterizing and classifying data flows related to each server application in said network, in combination with the other elements of the claims as a whole.

b. Regarding claims 41-50, 52-56, 59-69 and 71-75, the claims are allowable at least based on their dependence.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571)272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

August 31, 2011
/Michael J Simitoski/
Primary Examiner, Art Unit 2439